Nos. 23-2234(L), 23-2241(M)

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

HANAN ELATR KHASHOGGI,

Plaintiff-Appellant-Cross-Appellee,

v.

NSO GROUP TECHNOLOGIES LIMITED;
Q CYBER TECHNOLOGIES LIMITED,

Defendants-Appellees-Cross-Appellants.

On Appeal from the United States District Court Eastern District of Virginia, No. 1:23-cv-00779-LMB-LRV, Hon. Leonie M. Brinkema

---

OPENING/RESPONSE BRIEF FOR DEFENDANTS-APPELLEES-CROSS-APPELLANTS

-- REDACTED --

Joseph N. Akrotirianakis
Aaron Craig
Matthew H. Dawson
Matthew V.H. Noller
KING & SPALDING LLP
633 West Fifth Street
Suite 1600
Los Angeles, CA 90071
(213) 443-4355

Ashley C. Parrish
Edmund Power
KING & SPALDING LLP
1700 Pennsylvania Avenue NW
Washington, DC 20006
(202) 737-0500
aparrish@kslaw.com

Counsel for Defendants-Appellees-Cross-Appellants

May 22, 2024

CORPORATE DISCLOSURE STATEMENT

As required by Circuit Rule 26.1, Appellees/Cross-Appellants NSO Group Technologies Limited and Q Cyber Technologies Limited filed their Disclosure Statement on December 12, 2023. ECF 7.

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

Nos. 23-2234(L), 23-2241(M)

Caption: Hanan Khashoggi v. NSO Group Technologies Limited

Pursuant to FRAP 26.1 and Local Rule 26.1,

NSO Group Technologies Limited and Q Cyber Technologies Limited
(name of party/amicus)

who is Appellees/Cross-Appellants, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☑ YES ☐ NO
If yes, identify all parent corporations, including all generations of parent corporations:

NSO Group Technologies Ltd. is a privately owned corporation whose parent company is Q Cyber Technologies Limited, a privately owned corporation whose parent company is OSY Technologies S.à.r.l.

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☑NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/Ashley C. Parrish Date: 5/22/2024

Counsel for: Appellees/Cross-Appellants

Print to PDF for Filing

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

INTRODUCTION

Plaintiff Hanan Elatr Khashoggi contends that she was the victim of Saudi Arabia's and the United Arab Emirates' alleged persecution of the activist journalist Jamal Khashoggi. She alleges that the Saudi and UAE governments tried to monitor her communications with Mr. Khashoggi by installing on her mobile devices a technology manufactured by certain Israeli defense-technology manufacturers (collectively, "NSO"), who she has named as defendants in this action. That technology, called Pegasus, is essentially a high-tech wiretap that allows NSO's customers—who are always and exclusively vetted foreign governments and their agencies—to conduct law-enforcement and counterterrorism investigations. Plaintiff alleges that the UAE, acting on Saudi Arabia's behalf and in violation of its licensing agreement with NSO, misused Pegasus to monitor her phones while she was living in or visiting Dubai.

Plaintiff does not, however, sue Saudi Arabia or the UAE for her alleged harms. She plainly could not do so here, since those governments would be immune from suit as foreign sovereigns. So she sued NSO instead, claiming NSO should be liable for the UAE's alleged misuse of

Pegasus. But all NSO did was design Pegasus in Israel and then allegedly license Pegasus to the UAE. NSO had no knowledge that the UAE planned to misuse Pegasus to monitor Plaintiff's phones, as Plaintiff alleges. And once NSO licenses Pegasus to a foreign government, it plays no role in that government's uses of Pegasus. Just as a wiretap manufacturer does not itself listen to drug dealers' phone calls, and Lockheed Martin does not itself launch missiles, NSO itself does not install Pegasus on anyone's phone or access anyone's communications. And sure enough, Plaintiff's complaint does not allege that NSO played any role in installing Pegasus on her phones or intercepting her communications. She alleges only that the UAE or Saudi Arabia did so.

The district court correctly held that NSO cannot be sued in Virginia for the UAE's and Saudi Arabia's alleged conduct. The district court based its decision on a finding that Virginia courts cannot exercise personal jurisdiction over NSO. Plaintiff sued NSO in Virginia because she currently lives there, but she alleges no facts plausibly establishing that NSO directed any case-related conduct toward Virginia. *First*, Plaintiff does not allege that her phones were ever accessed in Virginia. She contends that she moved to Virginia no earlier than June 2018, *after*

the UAE allegedly tried to install Pegasus on her phones, and she never alleges that her phones were accessed in Virginia after that date. Nor could she, as undisputed evidence establishes that Pegasus cannot be used to monitor U.S. phone numbers or phones within the United States. *Second*, Plaintiff alleges that her phones were accessed only by the UAE or Saudi Arabia, not by NSO. She pleads no basis to attribute those third-party government's actions to NSO for purposes of personal jurisdiction. NSO's only alleged conduct—licensing Pegasus to the UAE—occurred overseas and had no connection to Virginia.

In any event, even if Plaintiff had alleged that NSO directed some case-related action toward Virginia, exercising personal jurisdiction over NSO would still be constitutionally unreasonable. As the district court found and Plaintiff does not dispute, NSO would be severely burdened by litigation in Virginia. It has no operations, offices, employees, witnesses, or evidence in Virginia, and it is subject to strict restrictions under Israeli law that would hamper its ability to participate in discovery or defend itself at trial. Any convenience to Plaintiff from litigating in Virginia cannot overcome these burdens.

For these reasons, this Court can and should affirm the district court's dismissal for lack of personal jurisdiction.

If the Court does not affirm for lack of personal jurisdiction, it should still affirm because there is no subject-matter jurisdiction. NSO is immune from suit under the common-law doctrine of conduct-based foreign sovereign immunity. To the extent Plaintiff contends that NSO played any role in the alleged monitoring of her phones, she alleges that it acted entirely as the agent of the UAE or Saudi Arabia. This Court has held that such agents of foreign governments are immune from suit. NSO's immunity, which the district court erroneously rejected based on nonbinding cases that conflict with this Court's precedent, provides an alternative basis for affirming the dismissal of Plaintiff's complaint.

JURISDICTIONAL STATEMENT

The district court lacked subject-matter jurisdiction over this action because NSO is immune from suit under the common-law doctrine of conduct-based foreign sovereign immunity. *See Butters v. Vance Int'l, Inc.*, 225 F.3d 462, 465-66 (4th Cir. 2000). The district court nonetheless asserted jurisdiction under 28 U.S.C. §§ 1331 and 1367(a), and properly

dismissed for lack of personal jurisdiction. This Court has appellate jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF ISSUES

1. Whether the district court correctly dismissed Plaintiff's complaint for lack of personal jurisdiction because Plaintiff pleads no facts establishing that the foreign Defendants directed any alleged case-related conduct at Virginia.

2. Whether the district court erred in concluding that NSO is not entitled to conduct-based foreign sovereign immunity when Plaintiff alleges that the Defendants acted exclusively as an agent of foreign governments, which this Court held confers immunity in *Butters v. Vance International, Inc.*, 225 F.3d 462 (4th Cir. 2000).

STATEMENT OF CASE

A. NSO's technology and its use in preventing terrorism and other serious crimes.

Defendant NSO is an Israeli company that designs, markets, and licenses a highly regulated cyber-security technology—known as "Pegasus"—exclusively to vetted foreign governments to assist in the investigation and prevention of terrorism and other serious crimes. JA11, JA93-95. Defendant Q Cyber, also an Israeli company, is NSO's sole

shareholder. JA11, JA93. The Israeli government strictly monitors and regulates the sale and export of NSO's Pegasus technology via Israel's Defense Export Control Law, and the Israeli Ministry of Defense determines the government agencies to which NSO may market or license its technology. JA94-95, JA98-129.

This lawsuit arises out of an alleged misuse of NSO's Pegasus technology. NSO does not, however, operate Pegasus—instead, NSO licenses the technology to foreign government agencies and installs the system for its clients' use. JA14, JA16-17, JA94-95. In short, NSO's government customers, not *NSO*, operate the technology and make all the decisions about how to do so. JA94-95. NSO generally has no knowledge of who its customers monitor and no access to the information that its customers collect. JA95-96. Moreover, NSO designs its technology solely for governments to use in investigating and preventing terrorism and other serious crimes—not unlike investigatory wiretaps on which the United States and other Western democracies lawfully rely.[1]

[1] *See* Dov Lieber et al., *Police Tracked a Terror Suspect—Until His Phone Went Dark After a Facebook Warning*, Wall St. J. (Jan. 2, 2020), https://on.wsj.com/38uXk5s (discussing European democracies' use of NSO's technology to investigate Islamic State terrorists).

Governments and their agencies have successfully used NSO's technology to thwart major terrorist attacks, identify and capture child sex abusers, break up criminal organizations and drug trafficking rings, and free kidnapping and human trafficking victims.[2]

NSO's license agreements prohibit its government customers from using the technology for any purpose other than the prevention and investigation of terrorism and criminal activity. JA94. If a foreign government were to misuse the technology beyond those purposes, it would do so in violation of its contract with NSO. JA94. NSO has also voluntarily undertaken additional steps to ensure that foreign governments use the Pegasus technology responsibly, including committing itself to the authoritative international standards of the United Nations' 2011 and 2023 Guiding Principles on Business and Human Rights and the Organization for Economic Cooperation and Development's Guidelines for Multinational Enterprises. *See* NSO Transparency Report at 9. Consistent with those standards, NSO

[2] NSO Grp., Transparency and Responsibility Report 2023 at 7-8 (Dec. 31, 2023) ("NSO Transparency Report"), *available at* https://www.nsogroup.com/wp-content/uploads/2023/12/2023-Transparency-and-Responsibility-Report.pdf.

conducts due diligence on all potential customers by, for example, examining publicly available information, evaluating questionnaires, and considering the potential customer's record of respecting rule-of-law concerns. JA95. NSO will not license its technology until it completes this due diligence review to NSO's satisfaction. JA95.

NSO's Pegasus technology is equipped with technical safeguards, such as general and customer-specific geographic limitations. JA95. As pertinent here, NSO's Pegasus technology cannot be used against U.S. mobile phone numbers or devices within the geographic bounds of the United States. JA95.

B. Israeli and foreign regulation of NSO's exports and operations.

The Israeli government strictly monitors and regulates NSO's activities with respect to Pegasus. JA93. Israel's Defense Export Control Law prohibits the distribution of "defense know how"—including information about Pegasus—outside Israel without a license from the Israeli government. JA93-94, JA98-129. The licensing process requires NSO to provide the Israeli Ministry of Defense with documents and information about NSO's prospective customers, the technology requested for export, and the intended uses for Pegasus (to confirm the

technology will only be used to investigate and prevent terrorism and criminal activity). JA93-94. Israel's Defense Export Control Law also empowers the Israeli Ministry of Defense to investigate NSO and its business, refuse or cancel NSO's registration as an exporter, grant or deny NSO's license (considering factors such as the intended use of NSO's technology and the identity of its customers), and revoke NSO's licenses entirely. JA93-94.

On July 19, 2020, [redacted] JA213. [redacted] JA213, JA216-219 (quotation marks omitted). [redacted] JA213, JA220-222. [redacted] JA220. [redacted]

[redacted] JA220. [redacted]

[redacted] JA213.

Separately, on November 4, 2021, the U.S. Department of Commerce restricted U.S. exports to NSO. *See* 15 C.F.R. § 744, Supp. 4. The Department's Bureau of Industry and Security ("the Bureau") entered NSO on its "Entity List," which prohibits any U.S. entity from exporting to NSO items subject to Export Administration Regulations. *See id.*; JA16. Under the governing regulations, "items" include hardware, software, technology, and related technical information that is currently located in—or comes into—the United States. 15 C.F.R. §§ 734.3(a)(1), 772.1. The Bureau may grant licenses authorizing the transfer of items to NSO otherwise subject to the regulations, but it has indicated that licenses requested for NSO will be subject to a presumption of denial. *Id.* § 744, Supp. 4.

In early 2023, NSO and its defense counsel sought export licenses from both the Israeli and U.S. governments. On February 21, 2023, King & Spalding applied to the Bureau for an export license so that it could discuss information about NSO's technology with NSO and prepare

NSO's U.S. litigation defense. JA130. The Bureau returned the license application without action. JA130. King & Spalding's subsequent discussions with the Bureau have not resulted in a license grant. JA130. On June 8, 2023, NSO applied to the Israeli Ministry of Defense for a license to export certain information related to Pegasus. JA96. To date, the Ministry has not granted NSO's request beyond limited disclosures to NSO's counsel of record, King & Spalding LLP. JA96.

The [redacted] in late July 2023. JA213-214. [redacted]. JA223-226. First, [redacted] JA224. Second, [redacted] JA224-225. Third, [redacted]

JA225. And NSO [redacted]. JA225-226.

C. Plaintiff's allegations of the UAE's "misuse" of NSO technology.

Plaintiff is an Egyptian citizen and currently a resident of the United States. JA9. She claims that Saudi Arabia and the UAE monitored her with Pegasus due to her relationship with Jamal Khashoggi, a deceased journalist and critic of the Saudi government. JA9.

Plaintiff, who previously lived in Dubai, worked as a flight attendant for Emirates Airlines for nearly 20 years, JA10, JA145. After meeting Mr. Khashoggi abroad and maintaining a friendship for nearly a decade, Plaintiff allegedly married Mr. Khashoggi in a religious (but not civil) ceremony in Virginia in June 2018. JA10. In October 2018, Mr. Khashoggi traveled to the Saudi consulate in Istanbul, Turkey, to collect documentation necessary to be married civilly to another woman, Hatice Cengiz. *Cengiz v. Salman*, 2022 WL 17475400, at *2 (D.D.C. Dec. 6, 2022). The Saudi government knew Mr. Khashoggi would be at the consulate because it instructed him to apply for the required documents there and because Mr. Khashoggi informed high-ranking Saudi officials

before arranging his visit. *Id.* at *2-3. While Mr. Khashoggi was at the consulate, Saudi agents—supposedly "assisted by allies in the [UAE]"—are alleged to have kidnapped and murdered him. JA9, JA34-35.

Plaintiff maintains that NSO bears responsibility for Mr. Khashoggi's death because NSO licensed its Pegasus technology to the UAE, which she alleges worked with Saudi Arabia to monitor her private communications with Mr. Khashoggi. JA26-35.

More specifically, Plaintiff alleges that "an agency of the UAE" sent her "a text message" containing "a disabled Pegasus link" in November 2017. JA30. Because the link was "disabled," however, Plaintiff does not—and cannot—allege that Pegasus was actually *installed* on any of her devices as a result of the UAE's text messages.[3] Instead, Plaintiff contends that, in April 2018, she received "more malicious text messages" and was later "detained" in Dubai by "Emerati intelligence officers" who "manually installed" Pegasus "onto at least one of her phones." JA31.

[3] According to public reporting Plaintiff incorporated in her complaint, "[a] forensic analysis of [her] Android phone … did not confirm whether the device had been successfully infected." Stephanie Kirchgaessner, *Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests*, Guardian (July 18, 2021), https://tinyurl.com/3fms4j32 (cited at JA35).

According to Plaintiff, the UAE took these steps to assist its "key ally," Saudi Arabia. JA31. Plaintiff does not allege any facts suggesting the NSO was involved in either government's alleged use of Pegasus.

Nor does Plaintiff allege that she lived in Virginia during any attempted installation of Pegasus on her phone or when her communications were allegedly monitored. Plaintiff alleges at most that she moved to Virginia no earlier than June 2018, JA10, and her own public statements confirm that she did not move to the United States until after *October* 2018. JA147. As the following table reflects, Plaintiff does not plausibly allege that anyone—much less NSO—accessed her phones while she lived in Virginia.

Timeline of Plaintiff's Residence		
Date	**Event**	**Residence**
November 2017	The UAE allegedly "attempts" to install Pegasus by sending Plaintiff "disabled Pegasus link[s]." JA30.	Dubai
April 2018	The UAE allegedly sends "more malicious text messages." JA31.	Dubai
April 2018	The UAE allegedly seizes Plaintiff and tries to "manually install[]" Pegasus on her phone. JA31.	Dubai

June-Oct. 2018	Plaintiff travels "often," while her communications with Mr. Khashoggi are allegedly "available to"—though not necessarily accessed by—the UAE. JA32-36.	Dubai
October 2018	Mr. Khashoggi is killed (JA34), and Plaintiff moves to Virginia after his death, JA145-147.	Virginia

D. Procedural Background

Plaintiff filed this lawsuit against NSO in June 2023, asserting claims under the federal Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, and Virginia tort law. JA7-88. NSO moved to dismiss on multiple distinct grounds: (1) the district court lacked subject-matter jurisdiction because NSO is immune from suit for actions that it allegedly took on behalf of foreign governments; (2) the district court lacked personal jurisdiction over NSO; (3) the act of state doctrine bars Plaintiff's claims; (4) Virginia was an improper forum under the doctrine of *forum non conveniens*; (5) Plaintiff's CFAA claim was time-barred; and (6) the Complaint did not state any claim for relief. Dkt. 26.

The district court granted NSO's motion. JA180. Although the court rejected NSO's immunity argument, it agreed that it could not exercise personal jurisdiction over NSO. JA187-202. It found that Plaintiff had

not made "any non-conclusory allegations regarding how long and where [she] had been living in [Virginia], and how NSO specifically participated in the surveillance of her phones while she was in Virginia, as opposed to conduct that may have occurred while she was overseas or traveling for work." JA194. In addition, the court determined that even if Plaintiff had alleged "that Pegasus was installed on her phones while she was in Virginia, or that Pegasus captured data from her phones while she was in Virginia," her own allegations established that "those actions were carried out by" the UAE or Saudi Arabia, not by NSO. JA195. As a result, the court concluded, Plaintiff had not adequately alleged that NSO "purposefully aimed its conduct at [P]laintiff in Virginia." JA197-198. The Court also held that exercising personal jurisdiction over NSO in Virginia would not be "constitutionally reasonable." JA200-201.

In the district court, Plaintiff never raised the argument she now presses on appeal—that "the place where unlawful interception of electronic data occurs is where the data is first captured and rerouted." Opening Br. 27 (emphasis omitted). To the contrary, "[w]hen asked in open court about how long [P]laintiff was living in Virginia," her counsel "was unable to link specific dates to specific alleged conduct by NSO."

JA195. Plaintiff argued only that her allegations "l[eft] open the 'possibility' that NSO Group purposefully targeted [P]laintiff while she was in Virginia." JA197; *see* JA158, JA160-161. As the district court recognized, "'possibility' is precisely the wrong standard" for personal jurisdiction. JA197. It held that because "Plaintiff does not plausibly allege any specific Virginia-related conduct by NSO," personal jurisdiction did not exist. JA198. And because Plaintiff "did not request leave to amend," the court dismissed her complaint with prejudice. JA203 n.15.

The district court did not address NSO's other arguments for dismissal, but it stated that NSO raised "strong arguments that a more appropriate forum for this civil action would be in Israel," that Plaintiff "likely fails to state claims upon which relief can be granted," and that Plaintiff's CFAA claim was "time barred." JA181 n.2; JA202 n.14. Those arguments would remain available to NSO if this Court were to remand.

Plaintiff appealed the dismissal of her complaint. JA207. NSO cross-appealed the district court's rejection of NSO's immunity argument. JA210.

SUMMARY OF ARGUMENT

1. The district court correctly held that it could not exercise personal jurisdiction over NSO in this case. NSO "is an Israeli corporation, which [P]laintiff is suing because it licensed its technology to foreign sovereigns that [P]laintiff alleges used the technology to monitor her devices." JA195. As the district court correctly found, Plaintiff alleges no facts plausibly suggesting that her phones were accessed or monitored *in Virginia*, let alone that *NSO* was responsible for any conduct directed toward Virginia.

The district court correctly found that Plaintiff does not allege that she lived in Virginia when her phones were allegedly accessed. To the contrary, she argues that she moved to Virginia in June 2018—*after* the UAE allegedly tried to install Pegasus on her phone. And for the period after June 2018, she does not allege that her phone was ever accessed while she was in Virginia as opposed to during the extensive periods when she was traveling to foreign countries as a flight attendant. Indeed, the undisputed evidence—which this Court may consider on a motion to dismiss for personal jurisdiction—reveals that Pegasus *could not* have

been used to access Plaintiff's phones while she was in Virginia or anywhere else in the United States. *See* JA95.

But even if Plaintiff *had* alleged that her phones were accessed in Virginia, she does not allege that *NSO* was responsible. To the contrary, she alleges only that *the UAE* and *Saudi Arabia* used Pegasus to access her phones. Her allegations about NSO are only general assertions about actions NSO *could* take in the abstract, none of which reflect any intentional targeting of Virginia. She never alleges that NSO took any of those actions *in this case*, let alone that it purposefully directed them toward Virginia. The only specific action that she alleges NSO took *in this case* was licensing Pegasus to the UAE, which occurred overseas and has no connection to Virginia. Under controlling precedent, NSO cannot be haled into court in Virginia for selling a technology overseas merely because a third-party government later unilaterally uses the technology to monitor someone.

The district court also correctly held that exercising personal jurisdiction over NSO would not be constitutionally reasonable. NSO, as a foreign entity with no operations, property, witnesses, or evidence in Virginia, would be subject to extreme burdens if this litigation were to

proceed, including onerous restrictions on discovery that would effectively prevent it from defending itself at trial. Moreover, this litigation presents severe threats to the sovereignty of Israel, which regulates, reviews, and approves the licensing decisions by NSO that Plaintiff challenges in this case. Plaintiff's convenience cannot overcome those burdens.

2. The district court also lacked subject-matter jurisdiction over this lawsuit. Because Plaintiff challenges NSO for actions that she claims it took on behalf of the UAE and Saudi Arabia, NSO is immune from suit under the common-law doctrine of conduct-based (or "derivative") sovereign immunity. This Court has extended that immunity to private entity contractors of foreign governments, and it applies with full force here. *Butters v. Vance Int'l, Inc.*, 225 F.3d 462, 465-66 (4th Cir. 2000).

The district court declined to follow *Butters* in light of the Ninth Circuit's holding that the Foreign Sovereign Immunities Act categorically forecloses common-law immunity for private entities. *See WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 17 F.4th 930 (9th Cir. 2021). But *WhatsApp* does not apply in this Circuit, and it is irreconcilable with this Court's binding decision in *Butters*. It is also poorly reasoned and unpersuasive on its own

terms. The district court's other ground for distinguishing *Butters*—that it applies only to *American* entities—is equally mistaken. Nothing in *Butters*'s text or logic excludes foreign entities from its scope, and any such restriction is inconsistent with the purpose of conduct-based immunity.

STANDARD OF REVIEW

This Court reviews a dismissal for lack of personal jurisdiction de novo, but it reviews "underlying factual findings for clear error." *Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.*, 334 F.3d 390, 396 (4th Cir. 2003). The Court reviews subject-matter jurisdiction de novo. *Tillman v. Resolution Tr. Corp.*, 37 F.3d 1032, 1034 (4th Cir. 1994).

When, as in this case, a defendant submits evidence along with a motion to dismiss for lack of personal or subject-matter jurisdiction, a court may consider that evidence and require the plaintiff to "prove the existence of personal jurisdiction by a preponderance of the evidence." *Grayson v. Anderson*, 816 F.3d 262, 268-69 (4th Cir. 2016).

ARGUMENT

The district court lacked both personal jurisdiction over NSO and subject-matter jurisdiction over the action. The court correctly dismissed Plaintiff's complaint on the former basis, but it erred in rejecting NSO's

argument on the latter. Accordingly, this Court should either affirm the district court's personal-jurisdiction dismissal (in Plaintiff's appeal) or order dismissal for lack of subject-matter jurisdiction (in NSO's cross-appeal). Either way, Plaintiff's claims cannot proceed.

I. The district court correctly dismissed Plaintiff's complaint for lack of personal jurisdiction.

Plaintiff seeks to sue a foreign company for its foreign conduct in designing a technology that foreign countries allegedly tried to use to monitor Plaintiff's devices abroad. That lawsuit does not belong in Virginia, as neither NSO nor its alleged suit-related conduct has any connection to Virginia. For that reason, the district court correctly held that it could not exercise personal jurisdiction over NSO.

"A federal district court may only exercise personal jurisdiction over a foreign corporation if such jurisdiction is authorized by the long-arm statute of the state in which it sits and application of the long-arm statute is consistent with the due process clause of the Fourteenth Amendment." *Consulting Eng'rs Corp. v. Geometric Ltd.*, 561 F.3d 273, 277 (4th Cir. 2009). Because "Virginia's long-arm statute is intended to extend personal jurisdiction to the extent permissible under the due process clause," the "constitutional inquiry" controls here. *Id.* And under the

Fourteenth Amendment, the district court could exercise personal jurisdiction over NSO only if NSO is subject to either general or specific jurisdiction in Virginia. *Carefirst*, 334 F.3d at 397. Because Plaintiff does not argue that NSO is subject to general jurisdiction in Virginia, Opening Br. 22, she must satisfy the requirements for specific jurisdiction.[4]

To meet that burden, Plaintiff must allege facts showing that her "claims arise out of" actions that NSO "purposefully directed" at Virginia. *Consulting Eng'rs*, 561 F.3d at 277-78 (cleaned up). In a case like this, in which Plaintiff bases her claims on alleged "Internet-based" conduct, she must establish that NSO "acted with the '*manifest intent*' of targeting" Virginia. *Carefirst*, 334 F.3d at 399-400 (emphasis added) (quoting *Young v. New Haven Advocate*, 315 F.3d 256, 264 (4th Cir. 2002)).

The district court correctly held that Plaintiff's allegations do not satisfy this test because she does not allege any conduct by NSO through which it intentionally targeted Virginia—let alone *manifestly* so. The district court also correctly held that, even if Plaintiff had alleged

[4] Plaintiff argued below that NSO was subject to nationwide jurisdiction under Federal Rule of Civil Procedure 4(k)(2), but she has waived that argument by not raising it in her opening brief in this Court. *E.g.*, *In re Apex Express Corp.*, 190 F.3d 624, 630 n.5 (4th Cir. 1999).

sufficient contacts between NSO and Virginia, the exercise of specific jurisdiction over NSO would not be "constitutionally reasonable." *Consulting Eng'rs*, 561 F.3d at 278. This Court should affirm those decisions.

A. NSO is not subject to specific jurisdiction in Virginia.

The district court correctly held that Plaintiff does not allege "sufficient, non-conclusory facts" to establish that NSO "intentionally directed" any suit-related conduct toward Virginia, "knowing that its conduct would cause harm to a forum resident." JA193-194 (citing *Calder v. Jones*, 465 U.S. 783 (1984)). As she did below, Plaintiff contends that NSO targeted Virginia "by accessing [her] devices there, obtaining her communications and data, and rerouting this information." Opening Br. 2. But as the district court recognized, Plaintiff's factual allegations do not support that conclusion. JA194-195.

1. Plaintiff does not plausibly allege that her phones were accessed in Virginia.

Plaintiff does not plausibly allege that she lived in Virginia when her phones were allegedly accessed. The absolute earliest her allegations suggest she moved to Virginia is June 2018. JA10 ¶ 15; Opening Br. 25. That means Plaintiff did not live in Virginia when the UAE allegedly sent

her a "text message" containing a "disabled Pegasus link" in November 2017. JA30 ¶¶ 101-03. She did not live in Virginia when the UAE allegedly sent her "more malicious text messages" in April 2018. JA31 ¶ 105. And she did not live in Virginia when the UAE allegedly "manually installed" Pegasus on her phone at the Dubai airport in April 2018—which did not take place in Virginia anyway. JA31 ¶ 106.

So even a generous reading of Plaintiff's complaint allows only a conclusion that she did not move to Virginia until *after* Saudi Arabia's and the UAE's alleged case-related conduct occurred. Indeed, Plaintiff's allegations clearly suggest that she did not "flee[] to the United States" until *after* the alleged "Pegasus attacks." JA39 ¶ 145. Her "unilateral" choice to move to Virginia after Pegasus was allegedly installed on her phone cannot support specific jurisdiction. *Walden v. Fiore*, 571 U.S. 277, 286 (2014); *see Farmers Ins. Exch. v. Portage La Prairie Mut. Ins. Co.*, 907 F.2d 911, 913 (9th Cir. 1990) ("Only contacts occurring prior to the event causing the litigation may be considered."); *accord Rossman v. State Farm Mut. Auto. Ins. Co.*, 832 F.2d 282, 287 n.2 (4th Cir. 1987).

Moreover, Plaintiff's own statements contradict any assertion that she moved to Virginia in June 2018. She has publicly stated that she did

not move to the United States until after Mr. Khashoggi's murder in October 2018, when she decided to seek asylum. JA147, JA199. The Court may consider those statements on a motion to dismiss for lack of personal jurisdiction, *Grayson*, 816 F.3d at 268-69, and Plaintiff has never submitted any contrary evidence. The record thus establishes that Plaintiff lived in Dubai in April 2018; *traveled* to Washington, D.C., in June 2018 to marry Mr. Khashoggi but "did not have residence in the U.S. at the time"; and moved to Virginia only *after* Mr. Khashoggi was killed in October 2018. JA145-147.

That is no doubt why her argument avoids any mention of her actual allegations of access, which all occurred between November 2017 and April 2018, before she moved to Virginia. *See* Opening Br. 25-26. Even after Plaintiff allegedly moved to Virginia, she "travel[ed] often" and was "home" only when "she was able to be." JA32 ¶ 111. She does not allege that she was in Virginia at any time her phones were allegedly accessed. And since the undisputed evidence below was that Pegasus *cannot* be used on phones within the United States, JA95, if her phones ever *were* accessed, it must have been while she was out of the country. Alleged conduct that occurred outside of Virginia, even if directed toward

a Virginia resident, does not "connect [NSO] to the forum in a meaningful way." *Walden*, 571 U.S. at 290. No matter when Plaintiff moved to Virginia, therefore, "none of [NSO's] challenged conduct had anything to do with [Virginia] itself." *Id.* at 289.

Even in Plaintiff's brief, she cannot cite a *single factual allegation* for her assertion that NSO "access[ed] [her] smartphones in Virginia." Opening Br. 25. She cites her conclusory "recitals of the elements of a cause of action," which "do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *see* Opening Br. 23 (citing JA38-41). Moreover, with one exception, those allegations do not even mention Virginia. JA38-41 ¶¶ 134-63. The one exception asserts in conclusory fashion that Plaintiff "liv[ed] in Virginia at the time Pegasus was installed on [her] devices," JA40 ¶ 155, which Plaintiff now admits is not true. She claims Pegasus was installed on her phones no later than April 2018, two months *before* she says she moved to Virginia. Opening Br. 6-7. The only other allegation she cites is a quotation from an unnamed source asserting (falsely) that NSO *in the abstract* receives information about its customers' uses of Pegasus. Opening Br. 23 (citing JA17 ¶ 46). But neither that allegation nor any other purports to describe anything NSO

did *with respect to Plaintiff*, let alone alleges that NSO accessed Plaintiff's phones in Virginia. *See Unspam Techs., Inc. v. Chernuk*, 716 F.3d 322, 329-30 (4th Cir. 2013) (holding allegations generally linking company to "many fraudulent prescription drug transactions" did not support personal jurisdiction when plaintiff did not "allege that [the company] was actually involved in [his] transaction").

Plaintiff does not allege a single fact plausibly suggesting that her phones were accessed in Virginia after she moved there. That is not an "inference against Plaintiff," Opening Br. 26 (emphasis omitted)—it is recognizing the utter lack of factual allegations that could support an inference *for* Plaintiff. That is particularly true in light of NSO's evidence that Pegasus *cannot* be used on U.S. phone numbers or within the United States, JA95, which Plaintiff has never contradicted. On a motion to dismiss for lack of personal jurisdiction, nothing precludes the district court or this Court from considering NSO's undisputed evidence in light of Plaintiff's failure to specifically allege that her phones were ever accessed in Virginia. *Grayson*, 816 F.3d at 268-69.

Plaintiff's argument that "the place where unlawful interception of electronic data occurs is where the data is first captured and rerouted,"

cannot rescue her complaint from dismissal. Opening Br. 27 (emphasis omitted). Plaintiff does not and cannot allege any facts establishing that her data *was* "first captured and rerouted" in Virginia as opposed to the UAE or any of the other locations Plaintiff traveled as a flight attendant. Moreover, Plaintiff waived this argument by not raising it in the district court. Dkts. 44, 45; JA150-179; *e.g.*, *Holland v. Big River Minerals Corp.*, 181 F.3d 597, 605 (4th Cir. 1999). It is disingenuous for Plaintiff to accuse the district court of "ignor[ing] authority" Plaintiff never cited. Opening Br. 27; *cf. Puckett v. United States*, 556 U.S. 129, 134 (2009) (requirement to preserve arguments "serves to induce the timely raising of claims and objections, which gives the district court the opportunity to consider and resolve them").

Plaintiff's supposed "authority" is irrelevant anyway. Neither *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016), nor *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022), had anything to do with personal jurisdiction. Both addressed only the meaning of specific statutory terms in state and federal wiretap statutes with no application to this case.

The plaintiff in *Luis* sued a technology company under the federal and Ohio Wiretap Acts for creating software that a jealous husband

installed on his wife's computer to collect his wife's communications with the plaintiff. 833 F.3d at 624. The company did not contest personal jurisdiction in Ohio or dispute that the software was installed on a computer in Ohio to collect communications received in and sent from Ohio. *See id.* at 623-24. Instead, the company argued (among other things) that only the husband "intercepted" the plaintiff's communications within the meaning of the relevant Wiretap Acts. *Id.* at 633. The Sixth Circuit rejected that argument in the portion of its opinion that Plaintiff quotes out of context, holding that the company itself could be liable because its "intercept[ion] of a communication … occur[ed] at the point where [the software]—without any active input from the user—captures the communication and reroutes it to [the company's] own servers." *Id.* That holding thus referred to the "point" at which communications were intercepted *temporally*—that is, whether before or after the user took any affirmative action to use the software. It had nothing to do with the *physical location* of an interception, much less the creation of contacts for purposes of personal jurisdiction.[5]

[5] The district court ultimately granted summary judgment to the company, finding that it did not "intercept" any of the plaintiff's

Popa, which arose on summary judgment rather than on a motion to dismiss, is equally irrelevant. The plaintiff there sued a website and a marketing service under Pennsylvania's Wiretapping and Electronic Surveillance Control Act for tracking her activities on the website. 52 F.4th at 124. The details of that tracking were fleshed out in detail by "testimony and evidence" in the summary judgment record. *Id.* at 124-25. The defendants argued that Pennsylvania law could not apply to their conduct because it occurred outside of the state. *Id.* at 130. The Third Circuit, in the portion of its opinion that Plaintiff cites, held that, *under the particular language of the Pennsylvania statute*, the interception occurred when the plaintiff's "browser accessed the [defendant's] website." *Id.* at 130-31. That interpretation of a specific Pennsylvania statute has no relevance to personal jurisdiction—and even if it did, it would not show that Plaintiff's own allegations establish that her phones were accessed in Virginia. Indeed, the Third Circuit could not determine from the record "where [the plaintiff's] browser accessed the [defendant's] website," so it remanded for further factfinding on that issue. *Id.* at 131-

communications, and the Sixth Circuit affirmed that decision. *Luis v. Zang*, No. 18-3707 (6th Cir. Apr. 19, 2019), ECF No. 19.

32. Here, by contrast, it was Plaintiff's burden to plead facts establishing that her phones were accessed in Virginia in a way that would create specific jurisdiction over NSO, and she has not done so. That requires dismissal even under Plaintiff's (erroneous) interpretation of *Popa*.

Plaintiff's reliance on irrelevant out-of-circuit cases is consistent with "the inaccurate way in which [her] briefing cite[d] authorities" below, and it "demonstrate[s]" the "weakness of [her] argument that the Court has personal jurisdiction over [NSO]." JA196. Plaintiff does not cite *any* case from *any* court exercising personal jurisdiction over a defendant based on allegations similar to hers. Nor does she address this Court's cases governing specific jurisdiction in cases based on alleged "Internet-based" conduct, which require factual allegations that the defendant "acted with the 'manifest intent' of targeting" Virginia. *Carefirst*, 334 F.3d at 399-400 (quoting *Young*, 314 F.3d at 265). Because none of Plaintiff's allegations establish that she was targeted in Virginia, she cannot satisfy that requirement. The district court correctly dismissed her complaint for that reason alone.

2. Plaintiff does not plausibly allege that NSO, as opposed to Saudi Arabia and the UAE, accessed her phones.

Plaintiff's claims also fail because she alleges no facts establishing that *NSO* was responsible for accessing her phones. To the contrary, the only potentially relevant conduct she describes was allegedly committed by Saudi Arabia or the UAE, not by NSO. JA198-200 & n.11. She alleges that "an agency of the UAE" texted her a "disabled Pegasus link," JA30 ¶ 102; that "Emirati intelligence officers" manually installed Pegasus on her phone, JA31 ¶ 106; that "Saudi Arabia … leveraged its relationship with a key ally, the United Arab Emirates, to install Pegasus on her phones," JA31 ¶ 108; and that her private communications were "relayed to the Saudis, via the UAE," JA33 ¶ 113, and "invaded by agents of an authoritarian government," JA37 ¶ 129. Therefore, the district court correctly concluded that Plaintiff "at best" alleges that NSO's "Pegasus technology infiltrated her devices only because of intervening acts by third-party sovereigns." JA199.

Such third-party actions cannot support specific jurisdiction over NSO. "[I]t is the defendant, not the plaintiff or third parties, who must create contacts with the forum State." *Walden*, 571 U.S. 277 at 291.

Accordingly, the "unilateral activity of … a third person is not an appropriate consideration when determining whether a defendant has sufficient contacts with a forum State to justify an assertion of jurisdiction." *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 417 (1984). It must be "the defendant *himself* that create[s] a 'substantial connection' with the forum State." *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) (quoting *McGee v. Int'l Life Ins. Co.*, 355 U.S. 220, 223 (1957)); *accord Fidrych v. Marriott Int'l, Inc.*, 952 F.3d 124, 143 (4th Cir. 2020).

Plaintiff pleads no basis to attribute Saudi Arabia's and the UAE's alleged conduct to NSO for purposes of specific jurisdiction. Plaintiff nowhere alleges that NSO knew the UAE or Saudi Arabia intended to monitor her (or any other Virginia resident) when NSO allegedly licensed Pegasus to the UAE. But even if she did, that would not support specific jurisdiction because a defendant's mere knowledge that the plaintiff lives in the forum state is not sufficient. *Walden*, 571 U.S. at 289; *Fidrych*, 952 F.3d at 140. As this Court has held, "a person cannot be haled into the forum simply because he knew that his conduct would have incidental effects there." *Hawkins v. i-TV Digitalis Tavkozlesi zrt.*, 935 F.3d 211,

230-31 (4th Cir. 2019). Instead, the defendant "must have 'expressly aimed' his conduct at the forum," and "mere knowledge of an incidental in-forum effect falls short of express aiming." *Id.* (quoting *Walden*, 571 U.S. at 288 n.7).

Likewise, Plaintiff does not allege that NSO influenced or had any "control over" the UAE's and Saudi Arabia's alleged decision to monitor her devices. *Farrar v. McFarlane Aviation, Inc.*, 823 F. App'x 161, 164 (4th Cir. 2020) (per curiam). She does not even allege that NSO *assisted* the UAE's and Saudi Arabia's claimed monitoring of her devices, beyond licensing its technology. She does not allege that NSO had any involvement in the UAE sending her infected text messages or installing Pegasus on her phone at the Dubai airport. JA30-31 ¶¶ 101-06. She simply asserts that NSO created the general infrastructure that allows Pegasus to function and that NSO, in the abstract, *can* assist its clients with set-up and technical support. Opening Br. 26-27. But NSO's initial creation of Pegasus and its infrastructure has no connection to Plaintiff or Virginia, and Plaintiff does not allege that NSO performed any support operations *for the UAE in connection with this case*—let alone that it purposefully targeted those operations at Virginia.

In any event, the simple "act of aiding and abetting … does not necessarily involve the sort of 'express aiming' at the forum that the effects test requires." *Hawkins*, 935 F.3d at 230-31. So even if Plaintiff *had* alleged that NSO assisted the UAE's or Saudi Arabia's alleged activities here, that still would not be enough to confer jurisdiction over NSO in Virginia.

For the same reasons, Plaintiff's allegations do not support her assertion that NSO *itself* "access[ed] [her] devices and obtain[ed] and rerout[ed] her information." Opening Br. 26-27. As just explained, the general allegations she cites address, at most, Pegasus's capabilities in the abstract. *See* JA17, JA67, JA69, JA70. They do not allege or suggest anything about what the UAE, Saudi Arabia, or NSO did *in this case* with respect to *Plaintiff's phones*. Specifically, NSO's general claim to operate in the fields of "cyber-intelligence, data acquisition, *and analysis*," Opening Br. 26 (emphasis in original) (quoting JA17), does not state that NSO itself analyzes data (as opposed to providing its customers data-analysis tools), does not indicate that the analysis is part of the Pegasus technology, describes nothing about what the analysis entails, and does not reflect anything about what services NSO allegedly provided the UAE. The

descriptions of Pegasus's capabilities, such as extracting calls or other communications and data, Opening Br. 26-27, reflect only what NSO's clients *can* use Pegasus to do, and not what anyone allegedly *in fact* did with respect to Plaintiff's phones. And the "anonymizing network" Plaintiff cites, Opening Br. 27, is part of the general Pegasus infrastructure, is not tied to any monitoring target or use of the technology, and does not provide NSO any information about targets or their data. It thus cannot establish purposeful direction toward any plaintiff or forum.

In addition, Plaintiff mischaracterizes the statements she cites. She quotes one sentence from a short 2019 description of NSO, which states that "NSO group is a global leader in the world of cyber-intelligence, data acquisition, and analysis."[6] That plainly does not say, as Plaintiff suggests, that NSO receives and analyses the data that its government customers collect using Pegasus. Instead, it is a general description of NSO's *entire* business, of which Pegasus is only one part. And while the

[6] *TeleStrategies ISS World Europe*, ISSWorldTraining.com (2019), *archived in* WayBackMachine (Sept. 8, 2019), https://web.archive.org/web/20190908051829/https://www.issworldtraining.com/iss_europe/sponsors.html.

alleged Pegasus brochure attached to Plaintiff's complaint describes Pegasus's "analysis" function, it makes clear that any analysis is conducted by the Pegasus *user*—that is, NSO's government customer—not by NSO itself. JA71-72.

Plaintiff also misquotes the alleged Pegasus brochure as claiming that NSO itself (as opposed to its government customers) can "obtain or extract the target's communications and data." Opening Br. 26 (citing JA67). That is not what the brochure says. The section Plaintiff quotes describes the applications (such as Skype and Viber) and categories of information (such as call histories and calendar information) that NSO's government customers can use Pegasus to access. JA65-67. The section concludes by explaining that certain customers may need data from "other applications … as time evolves and new applications are adopted by targets." JA67. Then follows the language Plaintiff quotes: "When such requirement is raised, we can fairly easily extract the important data from virtually any application upon customer demand and release it as a new release that will become available to a customer." JA67. In context, that language clearly means *only* that, when required by a particular government's investigatory needs, NSO can create new

versions of Pegasus that the government can use to access new applications or types of data. But "the user," not NSO, is always "the only one to decide when to conduct the upgrade." JA76. The brochure nowhere states that *NSO itself* will operate Pegasus to access any data stored on any target device. That is because, as NSO's unrebutted evidence shows, NSO does not operate Pegasus for its government customers nor does it collect information for its government customers. JA94-96.

Similarly, Plaintiff insinuates that NSO personally operates its "anonymizing network" for each use of Pegasus. Opening Br. 27 (quoting JA69-70). That is not correct. As explained above, the "anonymizing network" is a part of "[t]he Pegasus system," not tied to any specific use of the technology. JA69; *see* JA57 (describing the "Pegasus system," including the "Data Transmission" layer); JA79 (describing the anonymizing network). A Pegasus license includes the use of an anonymizing network, but once NSO licenses Pegasus to a customer it does not personally transmit or access any data over the network. JA94-96; *see* JA80 ("The above mentioned architecture allows *the operators* to issue new installations, extract, monitor and actively collect data from targets' devices." (emphasis added)). NSO's creation of technology that its

government customers can later use does not constitute purposeful direction of conduct toward any particular forum, much less toward Virginia. *E.g.*, *Farrar*, 823 F. App'x at 164; *see also St. Jarre v. Heidelberger Druckmaschinen, A.G.*, 19 F.3d 1430, 1994 WL 95944, at *3 (4th Cir. 1994) (per curiam) ("The exercise of personal jurisdiction over a foreign manufacturer, whose product reached the forum state because of intervening [acts] by third parties, would be unfair and unreasonable.").

3. NSO's alleged conduct was not purposefully directed toward Virginia.

The only alleged case-related conduct that Plaintiff attributes to NSO has no connection to Virginia. Plaintiff alleges that NSO licensed its Pegasus technology to the UAE, which then allegedly used Pegasus to monitor Plaintiff. But that licensing transaction would have occurred entirely overseas, meaning NSO did not "direct[] purposeful activity toward [Virginia] in relation to those particular sales." *Farrar*, 823 F. App'x at 164; *see also Unspam*, 716 F.3d at 328-29 (holding that foreign bank processing plaintiff's purchase in a foreign country did not support personal jurisdiction over bank in plaintiff's home forum of Virginia).

The alleged licensing, moreover, would have occurred well before the UAE allegedly used Pegasus to monitor any specific target, including

Plaintiff. JA23 ¶ 75 (alleging NSO licensed Pegasus to the UAE in 2016). Plaintiff does not allege that NSO knew when it licensed Pegasus that the UAE planned to monitor Plaintiff, much less that it licensed Pegasus to the UAE for the *purpose* of monitoring Plaintiff in Virginia. She alleges only that NSO knew or should have known about the UAE's alleged history of human rights abuses, which made her a "foreseeable victim of" the Pegasus "infrastructure." JA42 ¶ 168. That cannot show that NSO, by allegedly licensing Pegasus to the UAE, purposefully directed any actions toward Virginia. *E.g.*, *Walden*, 571 U.S. at 289; *Fidrych*, 952 F.3d at 140; *Hawkins*, 935 F.3d at 230-31.

As the district court recognized, NSO "is an Israeli corporation, which [P]laintiff is suing because it licensed its technology to foreign sovereigns that [P]laintiff alleges used the technology to monitor her devices." JA195. NSO's only alleged role in that conduct—its Israel-approved decision to license its technology to the UAE—occurred overseas and had no connection to Virginia. Exercising personal jurisdiction over such "purely foreign conduct" would violate due process and create "serious comity concerns." *Hawkins*, 935 F.3d at 231. The

district court correctly avoided that result by dismissing Plaintiff's complaint.

B. Exercising personal jurisdiction over NSO in Virginia would not be reasonable.

The district court also correctly held that exercising jurisdiction over NSO in Virginia would not "be constitutionally reasonable." *Consulting Eng'rs*, 561 F.3d at 278 (quotation marks omitted); JA200-202. That "constitutes an independent ground for dismissal," *Fed. Ins. Co. v. Lake Shore Inc.*, 886 F.2d 654, 661 (4th Cir. 1989), which this Court should affirm.

The district court properly concluded that "the factors counseling against personal jurisdiction being constitutionally reasonable are substantial." JA200. Those factors, including "(1) the burden on the defendant of litigating in the forum; (2) the interest of the forum state in adjudicating the dispute; (3) the plaintiff's interest in obtaining convenient and effective relief; (4) the shared interest of the states in obtaining efficient resolution of disputes; and (5) the interests of the states in furthering substantive social policies," *Consulting Eng'rs*, 561 F.3d at 279, strongly support the district court's decision.

Plaintiff does not dispute that the "burden" on NSO to litigate this suit in Virginia "would be considerable." *Fed. Ins.*, 886 F.2d at 661; *see* Opening Br. 34. As the district court found, NSO "is incorporated in Israel, owns no property in Virginia, and has no employees or persons authorized to act on its behalf in Virginia." JA200-201; *see* JA93. NSO thus has no "evidence or witnesses in Virginia." JA201. Any documents relevant to Plaintiff's allegations would be located in Israel or other foreign countries, and the testimony of current and former NSO employees in Israel would be required to address Plaintiff's allegations about NSO's technology and operations. Similarly, evidence and witnesses related to Plaintiff's alleged treatment by Saudi Arabia and the UAE would be located in those countries. The only Virginia witness is Plaintiff, and she cannot address any issues related to NSO's, the UAE's, or Saudi Arabia's alleged conduct. Those witnesses and evidence—the most important in the case—would primarily be "located in Israel, Saudi Arabia, and the UAE." JA201; *see* JA93, JA96. Courts routinely find personal jurisdiction unreasonable in similar circumstances. *E.g.*, *Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.*, 284 F.3d 1114, 1125-26 (9th Cir. 2002); *Fed. Ins.*, 886 F.2d at 661.

The Israeli Defense Export Control Law [redacted], along with NSO's presence on the Entity List, would impose substantial additional burdens on NSO if it were required to litigate this suit in Virginia. The [redacted]. JA225. [redacted]. JA217, JA220-221, JA223-224.

[redacted] Israel's Defense Export Control Law prohibits any Israeli citizen from "[t]ransfer[ring] … defense know-how through any means … from Israel to outside of Israel, or in Israel to a person who is neither an Israeli citizen [n]or an Israeli resident," unless the Israeli citizen has "received a license for such activity." JA114-115. The Defense Export Control Law defines "[d]efense know-how" as any "[i]nformation that is required for the development or production of defense equipment or its use, including information referring to design, assembly, inspection, upgrade and modification, training, maintenance, operation and repair of defense equipment or its handling in any other

way," including "technical data or technical assistance." JA100-101. Plaintiff's allegations focus on information about NSO's Pegasus technology that constitutes such "defense know-how." And any testimony about information covered by the Defense Export Control Law cannot lawfully be transferred "outside of Israel." JA114-115. Israeli witnesses may thus be unable to answer questions regarding NSO's technologies if those questions are asked by non-Israeli attorneys or their answers are at risk of being exported. JA134 ¶¶ 11-12; *see In re Factor VIII or IX Concentrate Blood Prods. Liab. Litig.*, 2008 WL 4866431, at *6 (N.D. Ill. June 4, 2008) (finding no "Israeli court [would] compel the appearance of an Israeli citizen for a deposition to be used in a trial to be conducted in the United States"). Without an export license, which NSO has not yet been able to obtain, the court and parties' access to critical documents and witnesses in Israel would be severely curtailed.

On the flipside, NSO's presence on the Commerce Department's Entity List would prevent U.S. individuals and entities from exporting various items to NSO. 15 C.F.R. § 744.11(a). The term "export" is defined broadly as any "transmission out of the United States … in any manner," including the "electronic transmission of non-public data that will be

received abroad." *Id.* §§ 730.5(c), 734.13(a)(1). The list of prohibited items includes both "software" and "technology." *Id.* §§ 772.1, 734.3(a)(1). "Technology" broadly includes any "[i]nformation necessary for the 'development,' 'production,' 'use,' operation, installation, maintenance, repair, overhaul, or refurbishing … of an item." *Id.* § 772.1. There is no exception for technology created and owned by NSO itself.

As a result, NSO's U.S. litigation counsel cannot communicate with NSO regarding NSO's own technology—the core subject matter of this litigation—or share with NSO substantial amounts of discovery that NSO would need to refute Plaintiff's allegations. Exports could be permitted with a license, but the U.S. government has indicated that any license application will face a "[p]resumption of denial." *Id.* § 744, Supp. 4. In fact, King & Spalding applied for a license so that it could defend NSO in other U.S. litigation, and the license was not granted. JA130 ¶ 2. Even NSO's e-discovery vendor was also unable to receive a license to provide NSO basic e-discovery technology. JA130-131 ¶ 3. In this age of electronic discovery, document review and production are all but impossible without e-discovery technology. Accordingly, if this

litigation were to proceed in Virginia, NSO's counsel would be unable to communicate fully with its clients about the case.

Although Plaintiff contends that her own interests favor jurisdiction in Virginia, Opening Br. 34, her "convenience alone cannot justify the heavy burden on [NSO] which the assertion of personal jurisdiction would impose." *Fed. Ins.*, 886 F.2d at 661. After all, "[d]ue process limits on the State's adjudicative authority principally protect the liberty of the nonresident defendant—not the convenience of the plaintiffs or third parties." *Walden*, 571 U.S. at 284; *see Grizzard v. LG Chem Ltd.*, 641 F. Supp. 3d 282, 292 (E.D. Va. 2022) (finding jurisdiction unreasonable even though "a number of … factors may point in [p]laintiff's favor"). Plaintiff's convenience is further limited by her failure to allege that she lived in Virginia when her devices were accessed. The only connection her claims have to Virginia is that she happens to live there now, which does not confer on Virginia or Plaintiff a strong enough interest to overcome the burden on NSO.

Any interests Virginia or Plaintiff have in this lawsuit proceeding in Virginia also pale in comparison to Israel's sovereign interests. The Supreme Court has warned that "great care and reserve should be

exercised when extending our notions of personal jurisdiction into the international field." *Asahi Metal Indus. Co. v. Super. Ct.*, 480 U.S. 102, 115 (1987) (cleaned up); *accord Hawkins*, 935 F.3d at 232. So "[w]here, as here, the defendant is from a foreign nation rather than another state, the sovereignty barrier is high and undermines the reasonableness of personal jurisdiction." *Amoco Egypt Oil Co. v. Leonis Navigation Co.*, 1 F.3d 848, 852 (9th Cir. 1993).

This lawsuit in particular threatens Israel's interests because the Israeli government regulates and reviews NSO's operations—including the licensing decisions that Plaintiff seeks to challenge under Virginia law—and details of Israel's decisions would have to be disclosed for NSO to defend this action [redacted] JA93-94, JA96, JA224-225.[7] [redacted].

[7] Plaintiff's claims also threaten the sovereignty of the UAE and Saudi Arabia, since she challenges actions allegedly conducted or ordered by those countries. *See Alhathloul v. DarkMatter Grp.*, 2023 WL 2537761, at *10 (D. Or. Mar. 16, 2023) (finding personal jurisdiction unreasonable because plaintiff's CFAA claims based on alleged hacking "relate[d] to conduct carried out at the behest of the UAE government" (quotation marks omitted)).

JA217, JA220-221, JA223-224. The Israeli Defense Export Control Law likewise reflects a strong national-security interest in the subject matter of this action, and it would prohibit NSO from producing broad swaths of information relevant to Plaintiff's claims. JA93-94, JA114-115.

Plaintiff primarily relies on the nonbinding decision in *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649 (N.D. Cal. 2020), but even if that decision had been correctly decided—and it was not—it does not support personal jurisdiction here. The court in *WhatsApp* exercised personal jurisdiction over NSO because WhatsApp alleged that NSO specifically targeted its California-based servers, including when it was researching and developing Pegasus. *Id.* at 670. Because WhatsApp was "allegedly harmed in California," the court concluded that California had "a strong interest" in the suit. *Id.* at 677. As explained above, Plaintiff makes no similar allegation that NSO accessed her phones in Virginia. In addition, because WhatsApp had conducted its own investigation into NSO's alleged access to its servers, WhatsApp had numerous "witnesses and evidence … located in California." *Id.* at 676. Here, in contrast, Plaintiff is the only Virginia-based witness. All other witnesses and evidence are in other forums, primarily Israel, the UAE, and Saudi

Arabia. JA201; *see also* JA136 (showing Plaintiff's declarant, Bill Marczak, lives in California).

At the time the *WhatsApp* court issued its decision, [redacted], JA217, JA220-221, JA223-224, [redacted] that would hamstring NSO if this litigation were to proceed. Nor, at that time, had the Department of Commerce placed NSO on the Entity List. The *WhatsApp* court thus could not consider those developments, which drastically reduce the reasonableness of exercising jurisdiction over NSO.

Whatever the court decided in *WhatsApp*, the circumstances of *this* case confirm the district court's holding that it could not reasonably exercise personal jurisdiction over NSO. This Court should affirm that decision.

II. The district court lacked subject-matter jurisdiction because NSO is immune from suit.

Although the district court correctly dismissed Plaintiff's claims for lack of personal jurisdiction, the court also lacked subject-matter jurisdiction under the common-law doctrine of conduct-based (or

"derivative") sovereign immunity. *See Butters*, 225 F.3d at 466. That form of immunity—which deprives federal courts of jurisdiction over suits challenging the actions taken by agents of foreign governments, *Yousuf v. Samantar*, 699 F.3d 763, 773-75 (4th Cir. 2012)—shields NSO from Plaintiff's allegations.[8]

To be clear, NSO was not involved in monitoring any of Plaintiff's devices. But to the extent Plaintiff claims otherwise, she alleges that NSO acted exclusively on behalf of Saudi Arabia and the UAE to assist those nations' sovereign activities. NSO cannot be sued for that alleged conduct on behalf of foreign governments, and the district court erred in holding otherwise.

A. Common-law immunity protects the private agents of foreign governments.

For more than 200 years, U.S. law has conferred common-law immunity on the officials and other agents of foreign states. *Samantar v. Yousuf*, 560 U.S. 305, 311-12, 321 (2010); *Yousuf*, 699 F.3d at 774-75. This "conduct-based immunity" turns on the nature of the agent's "act itself

[8] This Court may affirm the district court's personal-jurisdiction dismissal without reaching subject-matter jurisdiction. *Ruhrgas AG v. Marathon Oil Co.*, 526 U.S. 574, 584-85 (1999).

and whether the act was performed on behalf of the foreign state," not on the agent's identity. *Rishikof v. Mortada*, 70 F. Supp. 3d 8, 13 (D.D.C. 2014). As a result, "any act performed by the individual as an act of the State enjoys the immunity which the State enjoys." *Yousuf*, 699 F.3d at 774 (cleaned up).

Consistent with conduct-based immunity's focus on the nature of an agent's *act* rather than on the agent's identity, this Court has held that conduct-based immunity protects even *private entities* when they act as agents of foreign governments. *Butters*, 225 F.3d at 466. The plaintiff in *Butters* was a bodyguard whose employer had been hired by Saudi Arabia to protect a princess. At Saudi Arabia's request, the employer did not promote the plaintiff, who sued the employer. This Court held that the employer was derivatively immune as the "private agent[] of [a] foreign government." *Id.* It held, consistent with the common law, that "courts define the scope of sovereign immunity by the nature of the function being performed—not by the office or the position of the particular employee involved." *Id.* "All sovereigns," the Court recognized, "need flexibility to hire private agents to aid them in conducting governmental functions." *Id.* Therefore, private entity "agents enjoy

derivative sovereign immunity when following the commands of a foreign sovereign employer." *Id.*; *see also Velasco v. Gov't of Indonesia*, 370 F.3d 392, 398-99 (4th Cir. 2004) (recognizing *Butters* applied "foreign sovereign immunity" to agents "acting in [their] official capacity on behalf of a foreign state").[9]

Butters relied in part on *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379 (S.D. Tex. 1994). Two of the defendants in *Alicog* were private citizens who had been hired by Saudi Arabia to book hotel rooms and furnish drivers and security guards. *Id.* at 381. A Saudi prince ordered the private defendants to confine the plaintiffs, the prince's servants, to the prince's hotel. *Id.* at 384-85. The court held that the private defendants were immune for following the prince's orders because they were acting as Saudi Arabia's agents at the time. *Id.* The Fifth Circuit summarily affirmed. *Alicog v. Kingdom of Saudi Arabia*, 79 F.3d 1145 (5th Cir. 1996) (Table).

[9] Although *Butters* arguably grounded this immunity in the Foreign Sovereign Immunities Act, which this Court and the Supreme Court later held does not govern immunity for foreign agents, it remains "instructive for … questions of common law immunity." *Yousuf*, 699 F.3d at 774.

Other courts have reached the same conclusion. In *Moriah v. Bank of China*, 107 F. Supp. 3d 272 (S.D.N.Y. 2015), the court found a private Israeli citizen immune for actions he took "at the behest of the Israeli government." *Id.* at 277-78. Citing *Butters*, the court found it "well-settled" that "conduct-based immunity … extends beyond current and former officials to individuals acting as an agent for the government." *Id.* at 277 & n.34. And because the defendant acted at Israel's request, he was immune "as an agent of the Israeli government." *Id.* at 278. Similarly, the court in *Ivey ex rel. Carolina Golf Development Co. v. Lynch*, 2018 WL 3764264 (M.D.N.C. Aug. 8, 2018), relied on *Butters* to hold that a private attorney enjoyed common-law immunity for actions he took as the agent of a German official. *Id.* at *6-7. The court approved the defendant's argument that "foreign official immunity extends to the private, domestic agents of foreign officials." *Id.* (cleaned up).

Applying conduct-based immunity to the private agents of foreign states also accords with international law, which "has shaped the development of the common law of foreign sovereign immunity." *Yousuf*, 699 F.3d at 773. "'[C]ustomary international law'" has long granted immunity to "agent[s] for the government." *Moriah*, 107 F. Supp. 3d at

277 (quoting *Yousuf*, 699 F.3d at 774); *see Jones v. Ministry of Interior*, [2006] UKHL 26 ¶ 10 (H.L.) (appeal taken from Eng. and Wales); *Jaffe v. Miller*, [1993] 95 ILR 446, 460 (Can. Ont. C.A.). Under international law, therefore, "[t]he acts of [government] agents constitute direct State conduct and cannot be attributed as private activities to the person authorized to perform them." *Church of Scientology Case*, 65 ILR 193, 198 (Fed. Supreme Ct., Ger. 1978). That is true even when the agent is a private actor under the foreign state's laws. *Id.* at 197-98.

The international community has codified this consensus about the scope of conduct-based immunity in the U.N. Convention on Jurisdictional Immunities of States and their Property. U.N. General Assembly, *Resolution Adopted by the General Assembly on 2 December 2004*, U.N. Doc. A/59/38 (Dec. 16, 2004).[10] The Convention grants immunity to "representatives of the State acting in that capacity," including "entities" that "are entitled to perform and are actually performing acts in the exercise of sovereign authority of the State."

[10] *Available at* https://treaties.un.org/doc/source/docs/A_RES_59_38-E.pdf.

United Nations Convention on Jurisdictional Immunities of States and Their Property, art. 2, ¶ 1(b)(iii)-(iv), 2 December 2004.[11]

B. NSO is entitled to immunity under *Butters*.

Plaintiff's allegations trigger conduct-based immunity. Her entire case is based on allegations that the UAE used NSO's technology to monitor her devices on behalf of Saudi Arabia. *E.g.*, JA30-33 ¶¶ 101-03, 106-08, 113. But "a foreign government's deployment of clandestine agents to collect foreign intelligence on its behalf" is "peculiarly sovereign conduct" for which foreign governments are immune from suit. *Broidy Cap. Mgmt., LLC v. Qatar*, 982 F.3d 582, 595 (9th Cir. 2020). Under *Butters*, therefore, an agent who assists a foreign government's surveillance operations is likewise immune. 225 F.3d at 466.

While Plaintiff's complaint is silent on what, if anything, NSO allegedly did after licensing its technology to the UAE, it is clear that NSO would have taken any alleged actions on behalf of the UAE or Saudi Arabia. When generally describing NSO's business, Plaintiff alleges that NSO "assist[s]" and "support[s]" its government clients "after selling

[11] *Available at* https://treaties.un.org/doc/source/RecentTexts/English_3_13.pdf.

Pegasus to them." JA17 ¶¶ 45-46; JA22 ¶¶ 66-71. And when describing the actual alleged access to her devices, Plaintiff alleges that her "private communications" were intercepted "by *agents of an authoritarian government*." JA37 ¶ 129 (emphasis added). Plaintiff does not allege that NSO took any case-related action against her that was not conducted in its alleged role as an agent of the UAE or Saudi Arabia. For that reason, NSO is entitled to conduct-based immunity as an alleged "private agent[] of [a] foreign government." *Butters*, 225 F.3d at 466.

C. The district court erred in denying NSO immunity.

The district court held that NSO was not entitled to immunity under *Butters*. Instead, the district court followed the Ninth Circuit's nonbinding decision in *WhatsApp Inc. v. NSO Group Technologies Ltd.*, 17 F.4th 930 (9th Cir. 2021), which held that the Foreign Sovereign Immunities Act categorically forbids private entities from receiving common-law immunity. JA188-189. The court also held that *Butters* only protects American companies and does not apply to *foreign* agents of foreign governments. JA190. Each of those holdings was mistaken.

1. *Butters* precludes reliance on the Ninth Circuit's incorrect decision in *WhatsApp*.

The district court first erred by following the Ninth Circuit's decision in *WhatsApp* rather than *Butters*. Courts in this Circuit are bound by *Butters*, with which *WhatsApp* openly conflicts. But even if *Butters* did not foreclose reliance on *WhatsApp*, the Ninth Circuit's decision is incorrect and unpersuasive.

In *WhatsApp*, the Ninth Circuit held that no private entity can *ever* receive any form of common-law immunity. It based its decision on the fact that the Foreign Sovereign Immunities Act includes some state-owned entities within its definition of "foreign state[s]" entitled to foreign sovereign immunity. 28 U.S.C. § 1603(a)-(b); *see* 17 F.4th at 938-39. By doing so, the Ninth Circuit held the FSIA completely displaces common-law immunity for private entities: "an entity is entitled to foreign sovereign immunity, if at all, only under the FSIA. If an entity does not fall within the Act's definition of 'foreign state,' it cannot claim foreign sovereign immunity. Period." 17 F.4th at 937.

The district court endorsed that holding, JA188, but it is irreconcilable with *Butters*—as the Ninth Circuit itself recognized. *WhatsApp*, 17 F.4th at 939 n.6. *Butters* plainly granted to private entities

the conduct-based immunity that "agents enjoy … when following the commands of a foreign sovereign employer," a result that *WhatsApp* would forbid. *Butters*, 225 F.3d at 466. The Ninth Circuit thus openly rejected *Butters* as inconsistent with the proposition "that 'any sort of immunity defense made by a foreign sovereign in an American court must stand on the Act's text. Or it must fall.'" 17 F.4th at 939 n.6 (quoting *Rep. of Argentina v. NML Cap., Ltd.*, 573 U.S. 134, 141-42 (2014)). This Court, however, has never overruled *Butters*, so it remains binding precedent in this Circuit. *See K.I. v. Durham Pub. Schs. Bd. of Educ.*, 54 F.4th 779, 790 (4th Cir. 2022) ("A three-judge panel of this Court cannot overrule the decision of another panel."). The district court thus erred in following *WhatsApp* instead of *Butters*.

The Ninth Circuit's holding in *WhatsApp* is also unpersuasive and inconsistent with the Supreme Court's decision in *Samantar*. As *Samantar* held, the FSIA is a specific and narrow statute that governs only "whether a *foreign state* is entitled to sovereign immunity." 560 U.S. at 313 (emphasis added). Such foreign-state immunity is status-based: it depends on the *identity* of the defendant and, when it applies, is "virtually absolute." *Id.* at 311. The FSIA's definition of "foreign state" thus

incorporates entities that, because they are state-owned "agenc[ies] or instrumentalit[ies]," are equivalent to foreign states. *Id.* at 314; 28 U.S.C. § 1603(a)-(b). That definition limits only which entities possess near-categorical immunity based on their *status as foreign states*.

Common-law immunity, in contrast, depends on the defendant's *conduct* and is subject to limitations that do not apply to foreign-state immunity. *Samantar*, 560 U.S. at 321; *Yousuf*, 699 F.3d at 774. As *Samantar* held, the FSIA does not "supersede" such conduct-based immunity. 560 U.S. at 325. It "supersede[s] the common-law regime" only "for claims against *foreign states*." *Id.* (emphasis added). So, when a plaintiff sues a defendant that is not "a foreign state as the [FSIA] defines that term," the FSIA does not apply. *Id.* Those suits are "governed by the common law" alone. *Id.* And courts proceed "on the assumption that common-law principles of immunity were incorporated into our judicial system and that they should not be abrogated absent clear legislative intent to do so." *Filarsky v. Delia*, 566 U.S. 377, 389 (2012) (cleaned up).

For that reason, the Ninth Circuit and district court's focus on the FSIA's "comprehensive framework" misses the point. JA188. The FSIA is comprehensive only "if it applies." *Samantar*, 560 U.S. at 314. And it only

"applies" to "'foreign state[s],'" *id.*, which it defines to exclude private entities. So while it is true that "any sort of immunity defense *made by a foreign sovereign* in an American court must stand on the FSIA's text," JA190 (cleaned up) (emphasis added), that in no way suggests that the FSIA overrides the common law with respect to defendants, like NSO, that are *not* "foreign sovereigns."

Because NSO is not a "foreign state as the [FSIA] defines that term," the FSIA is simply irrelevant to whether it is entitled to immunity. *Samantar*, 560 U.S. at 325. Rather, as the D.C. Circuit has held, "claims of immunity" by "private entities" like NSO must "rise or fall not under the FSIA, but the residual law and practice that the FSIA did not displace." *Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789, 802 (D.C. Cir. 2021). Under *Butters*, that residual common law entitles NSO to immunity. 225 F.3d at 466.

2. *Butters* is not limited to American companies.

The district court further erred by holding that *Butters* applies only to *American* entities that serve as agents of foreign sovereigns. JA190. Although the agent in *Butters* happened to be an American company, this Court nowhere suggested that immunity turned on the agent's

nationality. *See Moriah*, 107 F. Supp. 3d at 277-78 (relying on *Butters* to immunize private Israeli citizen). To the contrary, this Court recognized that foreign sovereigns "need flexibility to hire private agents to aid them in conducting their government functions." *Butters*, 225 F.3d at 466. Conditioning immunity on whether a foreign state hired an American or foreign agent would limit that flexibility. And it would be quite odd for an immunity doctrine that protects *foreign* states and *foreign* agents to somehow exclude *foreign* entities.

If anything, American entities should be *less* entitled to conduct-based immunity than foreign entities. The United States has treated a defendant's U.S. residency as a reason to deny immunity because defendants "who enjoy the protections of U.S. law ordinarily should be subject to the jurisdiction of our courts." *Yousuf*, 699 F.3d at 767. That is all the more true of American corporations, which are not just protected by domestic law, but owe their very existence to it. *CTS Corp. v. Dynamics Corp.*, 481 U.S. 69, 94 (1987). This rationale for exercising jurisdiction over U.S. residents does not apply to foreign entities like NSO, which is a creature of Israeli law subject to extensive regulation in Israel. JA93-96 ¶¶ 4-10, 17.

The district court flipped this reasoning on its head, suggesting that immunity should uniquely encourage the use of American corporations to perform foreign contracts. JA190. But this protectionist "Buy American" rationale contradicts the "comity among nations" that underlies common-law immunity. *Yousuf*, 699 F.3d at 769. Just like the United States, foreign governments employ private contractors "to collect foreign intelligence on [their] behalf." *Qatar*, 982 F.3d at 595. Extending immunity to the American entities while withholding it from foreign entities hardly treats these foreign governments "as equals." *Jones*, UKHL 26 ¶ 1.

* * *

This case does not belong in Virginia. NSO is an Israeli corporation whose only alleged role in this case was licensing its technology to a foreign country that allegedly misused the technology to monitor Plaintiff. NSO's alleged conduct had no connection to Virginia, so it cannot constitutionally be sued for it in Virginia courts. Even if that were not so, this Court has recognized that alleged agents of foreign governments, such as NSO, cannot be sued in U.S. courts. For these reasons—plus others not yet addressed by the district court—Plaintiff's

complaint was properly dismissed. And it was properly dismissed with prejudice, because Plaintiff did not ask the district court for leave to amend and does not ask this Court to reverse the district court's denial of leave. JA203 n.15. This Court should affirm that decision.

CONCLUSION

This Court should affirm the dismissal of Plaintiff's complaint, either for lack of personal jurisdiction or, in the alternative, for lack of subject-matter jurisdiction.

Respectfully submitted,

s/Ashley C. Parrish

Ashley C. Parrish
Edmund Power
KING & SPALDING LLP
1700 Pennsylvania Avenue NW
Washington, DC 20006
(202) 737-0500
aparrish@kslaw.com

Joseph N. Akrotirianakis
Aaron Craig
Matthew H. Dawson
Matthew V.H. Noller
KING & SPALDING LLP
633 West Fifth Street
Suite 1600
Los Angeles, CA 90071
(213) 443-4355

Counsel for Defendants-Appellees-Cross-Appellants

May 22, 2024

STATEMENT REGARDING ORAL ARGUMENT

NSO believes the district court's dismissal for lack of personal jurisdiction is plainly correct and can be affirmed without oral argument. If the Court is inclined to grant oral argument on that issue, however, NSO respectfully requests oral argument on its cross-appeal from the district court's decision on subject-matter jurisdiction, which presents an important question under Fourth Circuit precedent that has divided the federal courts of appeal.

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B), because it contains 12,431 words, excluding the parts of the brief exempt by Federal Rule of Appellate Procedure 32(f).

This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6), because it has been prepared in a proportionally spaced typeface (14-point Century Schoolbook) using Microsoft Word 365 ProPlus.

Date: May 22, 2024

s/Ashley C. Parrish
Ashley C. Parrish

Counsel for Defendants-Appellees-Cross-Appellants